Experimental demonstration of in-service security monitoring using a quantum modulated signal

Yupeng Gong[1], Shuai Yang[1], Jeffrey. H. Hunt[2], Adrian Wonfor[1], Richard Penty[1] and Ian White[1,3]
[1]*Centre for Advanced Photonics and Electronics, 9 JJ Thomson Ave, University of Cambridge, Cambridge, CB3 0FA*
[2]*The Boeing company, Chicago, IL, US*
[3]*University of Bath, Claverton Down, Bath, BA2 7AY*
yg311@cam.ac.uk

Abstract: We experimentally demonstrate a method for in-service optical physical layer security monitoring with vacuum-noise sensitivity that can detect a 1% fiber tapping attack at 50km without classical security loopholes.

OCIS codes: Quantum communications (060.5565), Fiber optics communications (060.2330), Fiber measurements (060.2300)

1. Introduction

Nowadays, optical fiber networks are advancing rapidly to meet increasing capacity demands. Attack management and link security have become increasingly important for critical optical communication infrastructure. In addition to data encryption methods, classical physical layer security protection relies on active fiber monitoring techniques which are generally based on power monitoring and active diagnostics of the network [1], e.g. by measuring the optical mean power, or using optical time domain reflectometry (OTDR). However, such classical methods have vulnerabilities and security loopholes in practice [2]. They can, for example, be compromised by an intercept-resend attack. A sophisticated fiber tapping attack could perturb the fibre transmission by less than 1% [1], making real-time high-precision monitoring of the link power at the required precision challenging and costly.

Quantum key distribution (QKD) has been proven to be able to provide unconditional security for communication in terms of semantic security. This is guaranteed by quantum physics, such that legitimate users can detect the presence of any eavesdropper on the quantum communication channel [3]. This indicates that quantum physics can also provide physical layer security to a classical communication channel. In this paper, we experimentally demonstrate a quantum alarm (QA) monitoring system [4] which can provide in service surveillance of an optical network.

2. System set-up

In a method similar to that used in pilot tone systems, the link security is assured by sending special signals which here comprise continuous variable quantum states, i.e. weak coherent states modulated at the quantum level. They are sensitive to measurement in the channel so that, as any unauthorized measurement introduces extra noise, it can be detected. Both the quantum signal excess noise and channel loss can thus be precisely estimated and monitored by real-time processing of the quantum signals. This process is similar to the parameter estimation step in continuous variable (CV) QKD systems, which requires use of more than half the quantum states to characterize the link security and estimate the secure key rate. However, in a QA system, we employ all the quantum states simply for security monitoring.

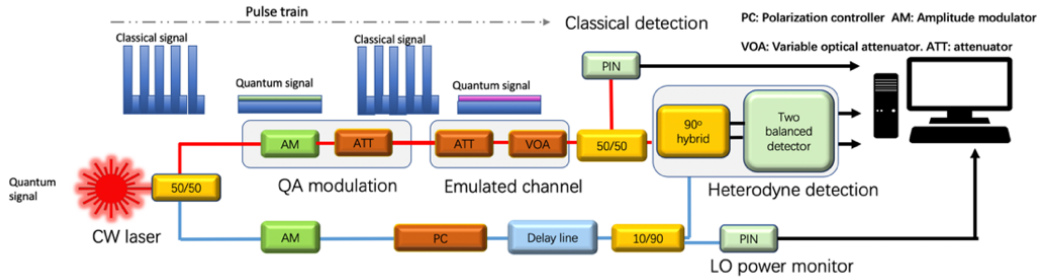

Figure 1: Block diagram of quantum monitored optical link

A diagram of the experimental set up is shown in Fig. 1. Here we randomly switch between sending classical modulated signals and quantum modulated signals using time division multiplexing (TDM) over the same channel with the same timeslot durations. For the classical signals, we encode random data using an on-off keying modulation scheme. For the quantum signals, we employ a two-state modulation scheme [5] that randomly sends one of two quantum states (namely state alpha and state beta) with the signal amplitude displaced to match the classical zero level. Hence, an eavesdropper cannot distinguish the quantum signals from the classical signal zero level.

For the signal preparation, we employ a single amplitude modulator to modulate both quantum and classical signals. A variable optical attenuator is used to emulate the optical channel with adjustable loss. At the receiver, a 50/50 splitter is used

to direct half of the received signals for classical signal detection, with the other half transmitted to the quantum receiver, which comprises two balanced homodyne detectors to measure both x and p quadratures of the signals. The quantum and classical measured results are both recorded by a personal computer (PC) for post-processing. In addition, for our initial demonstration, half of the power from the CW laser at the transmitter is pulsed and then connected to the quantum receiver as a local oscillator for homodyne measurement. In practice, this will be achieved by using a separate laser with the same wavelength at the receiver, similar to the architecture used in classical optical coherent communication systems and the local local oscillator CVQKD system proposed in [6]. In our tests, the system slot repetition rate is set as 25MHz, with the classical data rate set at 1Gbps.

3. Results and summary

We demonstrate our system performance under a correlated jamming attack. These attacks are especially demanding for classical attack detection techniques that are based on monitoring optical power as it maintains the optical power while monitoring part of the information. To implement the attack, we split off 1% of the signal and also re-inject light from another laser to maintain the same optical power before and after the attack. Hence, we combine both a 1% fibre tapping and also a jamming attack, while keeping the link power constant.

As can be seen from Fig.2, we perform the correlated jamming attack between data point 100 to 300. In Fig 2a we present the transmitted quantum signal, together with a smoothed 30 point moving average, for clarity. There is an obvious drop in the monitored quantum signal during the attack, despite the mean optical power remaining constant. The measured transmission is still decreased as the injected light cannot compensate the quantum signal. The transmission has a much larger fluctuation during the correlated jamming attack, since the measured standard deviation during the attack is about 0.009, i.e. 0.4dB, while that of a safe channel is less than 0.0015, i.e. 0.04dB. To avoid false alarms, we trigger the alarm when the moving average whose fluctuation is only 0.05% crosses the 1% threshold (at point 110). Based on the safe channel fluctuation, we can be 99.99% sure that it is caused by an eavesdropper.

In addition, Fig 2b shows the mean quantum excess noise, which increases from 0.14 shot noise units (snu) to 0.64 snu during the correlated jamming attack. This is equivalent to the OSNR decreasing by 1.5dB. We set the alarm threshold at the excess noise of 0.5 snu which is triggered at point 117. However, in practice, due to the sporadic nature of this attack, this extra noise and temporal BER drop is very hard to be detected classically. Nonetheless, the increase it causes in the quantum excess noise is easy to detect as it increases to nearly 5 times its original value. The quantum excess noise is calculated by removing the trusted noise from the measured quantum signal variance.

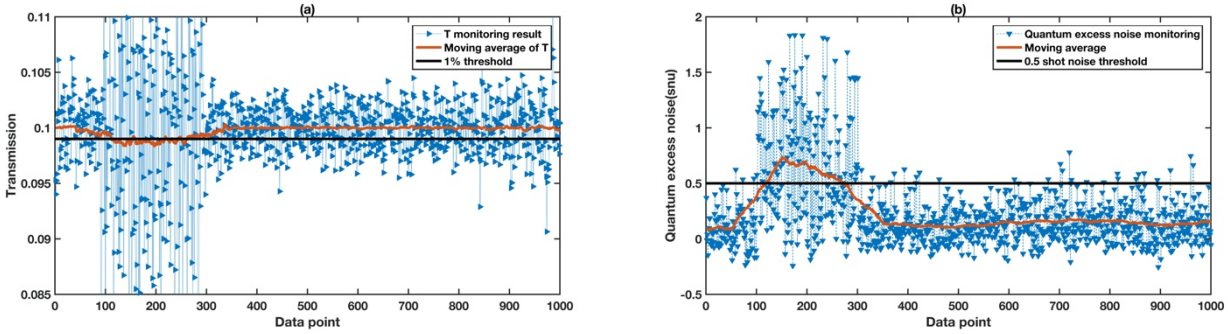

Figure 2: (a) Transmission monitoring result showing the moving average falling below the 1% trigger level (b) Quantum excess noise monitoring result

4. Conclusions

We demonstrate a Quantum Alarm which uses quantum states to monitor the classical channel security and detect a correlated jamming attack that is difficult to be detect by classical means. Our technique relies on quantum measurements and does not exhibit classical security loopholes., For example it outperforms classical loss monitoring, having a sensitivity of better than 0.04dB (at 50km) compared to 0.4dB using classical methods [7].

References

1. Skorin-Kapov, N., et al., *Physical-layer security in evolving optical networks.* IEEE Communications Magazine, 2016. **54**(8): p. 110-117.
2. Médard, M., P. Saengudomlert, and S. Chinn, *Attack detection in all-optical networks*. 1998.
3. Gisin, N., et al., *Trojan-horse attacks on quantum-key-distribution systems.* Physical Review A, 2006. **73**(2): p. 022320.
4. Gong, Y., et al. *Quantum monitored long-distance secure optical network*. in *Conference on Lasers and Electro-Optics*. 2018. San Jose, California: Optical Society of America.
5. Leverrier, A. and P. Grangier, *Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key Distribution with Discrete Modulation.* Physical Review Letters, 2009. **102**(18): p. 180504.
6. Qi, B., et al., *Generating the Local Oscillator ``Locally'' in Continuous-Variable Quantum Key Distribution Based on Coherent Detection.* Physical Review X, 2015. **5**(4): p. 041009.
7. Hui, R. and M. O'Sullivan, n *Fiber Optic Measurement Techniques*, Academic Press: Boston. p. 481-630.